Annual 47 C.F.R. § 64.2009(e) CPNI Certification Template

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

Date filed: **February 14, 2018**

Name of company(s) covered by this certification: **XIT Telecommunication & Technology, Ltd.**

Form 499 Filer ID: **818678**

Name of signatory: **Darrell F. Dennis**

Title of signatory: **General Manager**

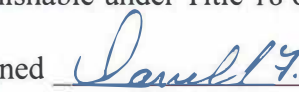
I, **Darrell F. Dennis**, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company ***has not*** taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. [NOTE: If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]

The company ***has not*** received customer complaints in the past year concerning the unauthorized release of CPNI. [NOTE: If you reply in the affirmative, provide a summary of such complaints. This summary must include the number of complaints, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed  [*Signature of an officer, as agent of the carrier*]
Darrell F. Dennis, General Manager

Attachments: Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers (if applicable)
Summary of customer complaints (if applicable)

XIT TELECOMMUNICATION & TECHNOLOGY, LTD.'S
STATEMENT OF COMPLIANCE WITH THE
FCC'S CPNI RULES

Pursuant to Section 64.2009(e) of the FCC's rules, this statement explains how XIT Telecommunication & Technology, Ltd.'s operating procedures ensure compliance with Part 64, Subpart U of the FCC rules on CPNI and its requirements for the safeguarding of such customer information.

The Company's CPNI Policy and Procedures manual describes what CPNI is, when it may be used without customer approval, and when customer approval is required. Disclosure of, or permitting access to customers' CPNI is not allowed without obtaining the requisite customer approval, except as required by law, or the exceptions set forth in 47 U.S.C. §222, and Subpart U of Title 47 of the Code of Federal Regulations; 47 C.F.R §64.2001 through §64.2011. The Company has chosen to prohibit the use of CPNI for marketing purposes by itself and between its affiliates. If customers' CPNI is to be used for sales and marketing campaigns in the future, the required notification will be provided to customers, approval obtained as required, and appropriate safeguards will be implemented in accordance with 47 C.F.R. §64.2009.

The Company has internal procedures in place to educate employees about CPNI and the disclosure of CPNI. Employees with access to this information are trained regarding the FCC's CPNI rules and are prohibited from disclosing or permitting access to CPNI without the appropriate customer consent or as allowed by law and the FCC rules. The Company has an express disciplinary process in place and the Company's CPNI Policy and Procedures Manual describes the disciplinary process for noncompliance with CPNI rules. Any employee that discloses, accesses, or uses CPNI without the appropriate customer consent is subject to disciplinary action, including possible termination.

The Company has designated a Director for CPNI Compliance who is responsible for: (1) communicating with the Company's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of Company employees who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to the Company's CPNI by independent contractors and joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Appropriate safeguards on the disclosure of CPNI have been implemented in accordance with C.F. R. §64.2010, including, but not limited to the following: Customers are properly authenticated before disclosing CPNI on customer-initiated telephone calls or business office visits. Authentication through the use of passwords and back-up authentication questions in the event of lost or forgotten passwords has been implemented. Passwords and back-up authentication questions are established in accordance with § 64.2010(e). For new customers, passwords and responses to back-up security questions are determined when the customer places an order to establish service. For existing customers to establish a password, the Company must first authenticate the customer without the use of readily available biographical or account information. This could be accomplished by calling the customer at the telephone number of record or reviewing a valid, photo ID if the customer comes to the business office.

Call detail information is only disclosed over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the Company asking for readily available biographical information or account information. If a customer does not provide a password, the Company only discloses call-detail information by sending it to the address of record or by calling the customer at the telephone number of record. Call detail information may be discussed if the customer is able to provide call detail information without the Company's assistance.

The Company's on-line system is designed to protect customers' CPNI from unauthorized access in accordance with § 64.2010(c) of the Commission's rules. Prior to allowing the customer online access to CPNI related to their telecommunications account, the customer is authenticated without the use of readily available biographical information or account information. Once authenticated, a customer can only access his/her online account through the use of a password that is not prompted by the Company asking for readily available biographical information or account information.

The Company has implemented procedures to notify customers immediately whenever a password, back-up means of authentication or address of record is created or changed.

The Company complies with the FCC's rules regarding the notification of law enforcement and customers, in the event of a CPNI breach. The Company maintains a record for at least two years of any breaches discovered, notifications made to law enforcement (i.e., United States Secret Service and the Federal Bureau of Investigation) and customers, and responses from law enforcement.